

AgentSPEX: A YAML Language for Specifying and Running AI Agent Workflows

Kabui, Charles

2026-04-30

[Read at ToKnow.ai](#)



AgentSPEX: A YAML Language for AI Agent Workflows

Declarative specification with typed steps, checkpointing, and verification

- 7** benchmarks across science, math, writing, and SWE
- 50+** tools in Docker sandbox via Model Context Protocol
- 12** typed workflow constructs with visual editor support

April 30, 2026

ToKnow.ai

Researchers at UIUC's ScaleML Lab released [AgentSPEX](#), a declarative YAML-based language for specifying AI agent workflows. The problem it solves: most agent systems today are tangled Python scripts where workflow logic (branching, looping, error recovery) is buried inside implementation code. AgentSPEX separates the two. You define what your agent does in a YAML file using 12 typed constructs (tasks, steps, if/switch, while, for_each, parallel, call,

and state operations), and a runtime engine handles execution inside a Docker-based sandbox with 50+ tools connected via Model Context Protocol. The system supports checkpointing after every step, meaning a workflow that fails mid-run can resume from where it stopped rather than restarting. A visual editor with synchronized graph and YAML views lets users build workflows by dragging nodes, with changes reflected in both directions instantly.

The practical value: a product manager or domain expert can read and modify an agent workflow in YAML without touching Python. The team evaluated AgentSPEX on 7 benchmarks spanning science, mathematics, writing, and software engineering, and ran a user study comparing it against a popular Python-based framework. Participants found AgentSPEX workflows significantly more interpretable and easier to modify. The formal verification angle is early-stage but promising: because control flow and variable dependencies are explicit in the YAML, you can define pre/post-conditions per step and verify them in Lean or Isabelle.

The broader pattern here: as AI agents move from demos to production, the ad-hoc “write a prompt and hope” approach is giving way to proper software engineering. AgentSPEX treats agent workflows like [infrastructure-as-code](#), something you version-control, diff, test, and share.

Sources:

- [AgentSPEX: An Agent Specification and Execution Language \(arXiv\)](#)
- [AgentSPEX GitHub Repository](#)
- [AgentSPEX Official Website](#)

*Disclaimer: For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation. **Read more:** [/terms-of-service](#)*